

#3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Hideyuki HIRANO, et al.

Application No.: To be Assigned

Filed: March 20, 2001

For: DATA ADMINISTRATION METHOD

Group Art Unit: To be Assigned

Examiner: To be Assigned

1c996 U.S. PTO
09/01/550
03/20/01

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

*Assistant Commissioner for Patents
Washington, D.C. 20231*

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s)
herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-342753
Filed: November 10, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing
date as evidenced by the certified papers attached hereto, in accordance with the requirements
of 35 U.S.C. §119.

Respectfully submitted,
STAAS & HALSEY LLP

By: _____
James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500
Date: 3/19

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

JC996 U.S. PRO
09/811550
03/20/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

2000年11月10日

出 願 番 号
Application Number:

特願2000-342753

出 願 人
Applicant(s):

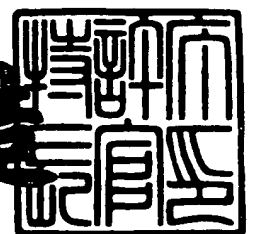
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 1月26日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3001648

【書類名】 特許願

【整理番号】 0095352

【提出日】 平成12年11月10日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 3/00

【発明の名称】 データ運用方法

【請求項の数】 10

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 平野 秀幸

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 橋本 晋二

【発明者】

【住所又は居所】 静岡県静岡市南町18番1号 株式会社富士通静岡エンジニアリング内

【氏名】 服部 衛紀

【発明者】

【住所又は居所】 静岡県静岡市南町18番1号 株式会社富士通静岡エンジニアリング内

【氏名】 望月 重利

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100094145

【弁理士】

【氏名又は名称】 小野 由己男

【連絡先】 0 6 - 3 5 5 - 5 3 5 5

【選任した代理人】

【識別番号】 100094167

【弁理士】

【氏名又は名称】 宮川 良夫

【選任した代理人】

【識別番号】 100106367

【弁理士】

【氏名又は名称】 稲積 朋子

【手数料の表示】

【予納台帳番号】 020905

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9807456

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ運用方法

【特許請求の範囲】

【請求項 1】

配布を行うデジタルコンテンツを暗号化して実データ部を作成し、前記デジタルコンテンツの属性を視覚的または聴覚的に認識できるようにシンボル化したシンボル情報を備える見出しデータ部を作成し、前記デジタルコンテンツの暗号化の際に暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を電子透かしとして前記見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成してこれを配布するデータ運用方法。

【請求項 2】

前記見出しデータ部は、複数のデジタルコンテンツにそれぞれ対応してその属性を視覚的に認識できるようにシンボル化された 1 つ以上の画像シンボルデータを、1 つの画像データ内に合成してなる、請求項 1 に記載のデータ運用方法。

【請求項 3】

配布を行うデジタルコンテンツを暗号化して実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータに前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記デジタルコンテンツの利用制限を行うための利用制限情報を暗号化した付属データ部を作成し、前記実データ部と前記許諾情報付見出しデータ部とを合成する際に前記付属データ部を同時に合成して合成データを作成してこれを配布するデータ運用方法。

【請求項 4】

前記利用制限情報は、前記許諾情報を前記見出しデータ部に電子透かしとして埋め込む際の埋込ロジックである、請求項 3 に記載のデータ運用方法。

【請求項 5】

配布を行うデジタルコンテンツを暗号化した実データ部と、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部に、前記見出しデータに前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部と、

前記デジタルコンテンツの利用制限を行うための利用制限情報を暗号化した付属データ部と、

を合成して配布される合成データから付属データ部を分離し、前記付属データ部を復号化して利用制限情報を取り出し、前記利用制限情報に基づいて前記許諾情報付見出しデータ部に埋め込まれた許諾情報を取り出し、前記許諾情報から前記デジタルコンテンツを復号化するためのコンテンツ鍵を取得し、このコンテンツ鍵を用いて前記実データ部を元のデジタルコンテンツに復号化して利用者に利用させるデータ運用方法。

【請求項 6】

配布を行うデジタルコンテンツを暗号化した実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部からハッシュ関数を用いて生成されたハッシュ値を、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ後、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成してこれを配布することを特徴とするデータ運用方法。

【請求項 7】

配布を行うデジタルコンテンツを暗号化した実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号

化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部をデジタルコンテンツに復号化する際に、所定の連絡先に回線接続して、復号化を行うデジタルコンテンツのコンテンツ情報を送出するために、前記デジタルコンテンツのコンテンツ情報と、前記所定の連絡先情報とを、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ後、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成してこれを配布することを特徴とするデータ運用方法。

【請求項 8】

配布を行うデジタルコンテンツを暗号化した実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成する際に、前記デジタルコンテンツを登録しているサーバの記録場所情報を、前記合成データ中に保持させ、この合成データを配布することを特徴とするデータ運用方法。

【請求項 9】

配布を行うデジタルコンテンツを暗号化した実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成する際に、前記デジタルコンテンツの利用者の生体情報に基づいて生成された

生体テンプレート情報を前記合成データ中に保持させ、この合成データを配布することを特徴とするデータ運用方法。

【請求項 1 0】

前記生体テンプレート情報を、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込むことを特徴とする、請求項 9 に記載のデータ運用方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、データ運用方法に関し、特に、デジタルコンテンツを暗号化して配布する際のデータ運用情報に関する。

【0 0 0 2】

【従来の技術】

コンピュータプログラムなどのソフトウェアや電子出版物では、光磁気ディスク（MO）、デジタルビデオディスク（DVD）、フロッピーディスク（FD）、ミニディスク（MD）、その他の記録媒体上に電子化データを格納して販売される。このような電子化データは、一般にコピーが容易であり、不正コピーが頻繁に行われている。このため、ソフトウェアベンダーや出版者側の著作権が侵害され著しく利益が阻害されるおそれがある。

【0 0 0 3】

また、インターネットやCATV、その他のネットワークなどを通じて配布される静止画像データ、動画データ、音声データ、音楽データを含む電子化データについても同様にして不正コピーが頻繁に行われ、著作権者の利益が損なわれている。

【0 0 0 4】

このような記録媒体上に格納された電子化データや各種ネットワークを通じて配布される電子化データなどのいわゆるデジタルコンテンツを保護するために、暗号鍵を用いてデジタルコンテンツを暗号化しこの暗号化された実データを配布することが行われる。

【 0 0 0 5 】

たとえば、ユーザが自分のパーソナルコンピュータからコンテンツの配布者側にアクセスを行い、デジタルコンテンツをハードディスク上にダウンロードを行ってこれを利用する場合を考える。まず、ユーザはホストコンピュータにアクセスしてダウンロードのためのプラグインモジュールを入手する。この後、使用しているハードディスクドライブの識別番号、使用しているコンピュータのCPU識別番号、その他ユーザ固有の識別情報をホストコンピュータ側に送付する。

【 0 0 0 6 】

コンテンツの配布者側では、デジタルコンテンツをコンテンツ鍵で暗号化した実データと、コンテンツ鍵をユーザ固有の識別情報で暗号化した許諾情報を、ユーザ側に送信する。

【 0 0 0 7 】

ユーザ側では、送られてきた暗号化実データと、許諾情報とを暗号化された状態のままハードディスクに記録する。デジタルコンテンツを利用する場合には、ハードディスクドライブの識別番号などのユーザ固有の識別情報を用いて、許諾情報を復号化し、コンテンツ鍵を取得する。このコンテンツ鍵を用いて、暗号化されたデジタルコンテンツを復号化してこれを利用する。

【 0 0 0 8 】

この場合、ユーザ個々にデジタルコンテンツの利用権を与える際に、デジタルコンテンツを暗号化するための暗号鍵を共通にすることができ、ユーザ毎に異なるユーザ固有の情報を用いて復号鍵を暗号化することによって、利用権を個々に与えることが可能となる。

【 0 0 0 9 】

【発明が解決しようとする課題】

上述の方法でデータの配布を行う場合、データ配布者は暗号化されたデジタルコンテンツと、暗号化されたデジタルコンテンツの復号鍵となる許諾情報とを別々に送付する必要がある。

【 0 0 1 0 】

また、ユーザ側においても、送付されてくる暗号化されたデジタルコンテンツ

とその許諾情報とを別々に記録媒体に格納しておく必要がある。

したがって、データ配布者側からユーザ側に送付される途中で許諾情報が破壊されたり、またはユーザ側の記録媒体上で許諾情報がなんらかの事故により破壊もしくは紛失した場合には、デジタルコンテンツを利用することができなくなり、再度許諾情報を入手する手順が必要となる。

【0011】

また、図書館の写本、美術館所蔵品などを写真やスキャナなどで画像データとして取り込み、これをユーザに利用させる場合、画像データが完全に暗号化されていると許諾情報のやりとりを行う前に、ユーザ側で所望の画像データを特定することが困難である。したがって、画像の一部がユーザ側で確認でき、かつ不正に流用されることがないように運用することが望ましい。

【0012】

静止画像、動画像などの画像データのみならず、音声データや音楽データなどを暗号化して配布する場合においても、どのようなデジタルコンテンツが含まれているかを視覚的または聴覚的に確認できるようにしておくことで、利用者にとって便利になる。

【0013】

本発明は、デジタルコンテンツを暗号化して配布することで著作権の侵害を防止するとともに、データ中に含まれているデジタルコンテンツがどのような内容であるかを把握することが容易であるようなデータ運用方法を提供する。

【0014】

【課題を解決するための手段】

本発明に係るデータ運用方法は、配布を行うデジタルコンテンツを暗号化して実データ部を作成し、デジタルコンテンツの属性を視覚的または聴覚的に認識できるようにシンボル化したシンボル情報を備える見出しデータ部を作成し、デジタルコンテンツの暗号化の際に暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を電子透かしとして見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成してこれを配布する。

【 0 0 1 5 】

ここで、見出しデータ部は、複数のデジタルコンテンツにそれぞれ対応してその内容を視覚的に認識できるようにシンボル化された1つ以上の画像シンボルデータを1つの画像データ内に合成して構成することができる。

【 0 0 1 6 】

また、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化して実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、デジタルコンテンツの利用制限を行うための利用制限情報を暗号化した付属データ部を作成し、実データ部と許諾情報付見出しデータ部とを合成する際に付属データ部を同時に合成して合成データを作成してこれを配布する。

【 0 0 1 7 】

このとき、利用制限情報として、許諾情報を前記見出しデータ部に電子透かしとして埋め込む際の埋込ロジックを用いることができる。

また、利用制限情報は、デジタルコンテンツを利用可能な利用期限または利用回数に基づくものとすることができる。

【 0 0 1 8 】

さらに、利用制限情報は、デジタルコンテンツの利用者の個人情報を暗号鍵として暗号化することができる。

この利用制限情報を暗号化する際の暗号鍵は、利用者によって予め設定されたパスワードとすることができ、合成データが記録される記録媒体に固有の識別情報とすることもでき、利用者の生体情報を用いることも可能である。

【 0 0 1 9 】

本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化した実データ部と、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部に、デジタルコンテンツを暗号化する際の暗号鍵として用い

たコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部と、デジタルコンテンツの利用制限を行うための利用制限情報を暗号化した付属データ部とを合成して配布される合成データから付属データ部を分離し、付属データ部を復号化して利用制限情報を取り出し、利用制限情報に基づいて許諾情報付見出しデータ部に埋め込まれた許諾情報を取り出し、許諾情報からデジタルコンテンツを復号化するためのコンテンツ鍵を取得し、このコンテンツ鍵を用いて実データ部を元のデジタルコンテンツに復号化して利用者に利用させる。

【 0 0 2 0 】

また、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化して実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、見出しデータ部にデジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、実データ部からハッシュ関数を用いて生成されたハッシュ値を、見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ後、実データ部と許諾情報付見出しデータ部とを合成した合成データを作成してこの合成データを配布する。

【 0 0 2 1 】

さらに、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化して実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報と、記録される記録媒体に固有の識別情報とを視覚的または聴覚的に認識不能な電子透かしとして見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、実データ部と許諾情報付見出しデータ部とを合成した合成データを作成して、この合成データを配布する。

【 0 0 2 2 】

また、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化し

て実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報と、デジタルコンテンツを再生するための情報機器に特定の動作をさせる制御コードとを視覚的または聴覚的に認識不能な電子透かしとして見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、実データ部と許諾情報付見出しデータ部とを合成した合成データを作成して、この合成データを配布する。

【 0 0 2 3 】

さらに、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化した実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、見出しデータ部にデジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、実データ部をデジタルコンテンツに復号化する際に、所定の連絡先に回線接続して、復号化を行うデジタルコンテンツのコンテンツ情報を送出するために、デジタルコンテンツのコンテンツ情報と、所定の連絡先情報とを、見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ後、実データ部と許諾情報付見出しデータ部とを合成した合成データを作成し、この合成データを配布する。

【 0 0 2 4 】

また、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化した実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、見出しデータ部にデジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、実データ部と許諾情報付見出しデータ部を合成した合成データを作成する際に、デジタルコンテンツを登録しているサーバの記録場所情報を、合成データ中に保持させ、この合成データを配布する。

【 0 0 2 5 】

ここで、デジタルコンテンツを登録しているサーバの記録場所情報を、見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込むことができる。

【 0 0 2 6 】

さらに、配布を行うデジタルコンテンツを暗号化した実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、見出しデータ部にデジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、実データ部と許諾情報付見出しデータ部を合成して合成データを作成する際に、デジタルコンテンツの利用者の生体情報に基づいて生成された生体テンプレート情報を、合成データ中に保持させ、この合成データを配布する。

【 0 0 2 7 】

ここで、生体テンプレート情報を、見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込むことができる。

また、本発明のデータ運用方法は、配布を行うデジタルコンテンツを暗号化した実データ部を作成し、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、見出しデータ部にデジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、実データ部と許諾情報付見出しデータ部を合成して合成データを作成し、この合成データを配布するものであって、デジタルコンテンツの著作権情報や版權情報を含む権利情報を、デジタルコンテンツ中に電子透かしとして埋め込む。

【 0 0 2 8 】

この場合、デジタルコンテンツに要求されるデータ品質レベルとセキュリティレベルとに基づいて、デジタルコンテンツ中に埋め込む電子透かしの形態と暗号化レベルを決定するように構成できる。

【 0 0 2 9 】

また、デジタルコンテンツ中への電子透かしの埋め込み方式と、見出しデータ部への電子透かしの埋め込み方式が異なる構成とすることができる。

【 0 0 3 0 】

【発明の実施の形態】

〔発明の概要〕

図 1 に本発明の概要構成を示す。

【 0 0 3 1 】

コンテンツ提供者 1 は、デジタルコンテンツの著作者、版權者などであり、運用を行うデジタルコンテンツ 1 1 をコンテンツ管理者 2 に提供する。

コンテンツ管理者 2 は、コンテンツ提供者 1 から提供されるデジタルコンテンツ 1 1 を運用するために暗号化し、暗号化する際の暗号鍵として用いたコンテンツ鍵を管理するとともに、このデジタルコンテンツ 1 1 を利用するユーザの利用者情報を管理する。

【 0 0 3 2 】

コンテンツ利用者 3 は、コンテンツ管理者 2 が管理しているデジタルコンテンツを利用したい場合には、利用者情報 1 4 をコンテンツ管理者 2 に送信する。

コンテンツ管理者 2 は、コンテンツ利用者 3 から送信された利用者情報 1 4 を管理するとともに、この利用者情報 1 4 に基づいて許諾情報 1 3 を作成し、デジタルコンテンツを暗号化した実データ部 1 5 と許諾情報 1 3 とを含む合成データ 1 2 をコンテンツ利用者 3 に送信する。

【 0 0 3 3 】

このとき、コンテンツ管理者 2 はデジタルコンテンツ 1 1 の属性を視覚的または聴覚的に認識できるようにシンボル化したシンボル情報を用いて見出しデータ部 1 6 を作成する。デジタルコンテンツ 1 1 を暗号化する際に用いたコンテンツ鍵を利用者情報 1 4 によって暗号化して許諾情報 1 3 を作成し、これを見出しデータ部 1 6 に電子透かしとして埋込んだ許諾情報付見出しデータ部を作成する。さらに、デジタルコンテンツを暗号化した実データ部 1 5 と許諾情報付見出しデータ部とを合成してコンテンツ利用者 3 に送信する。

【 0 0 3 4 】

合成データ部 1 2 は、図 2 に示すように、見出しデータ部 1 6 と、暗号化された実データ部 1 5 が合成されたデータ構成となる。許諾情報を電子透かしとして見出しデータ部 1 6 に埋め込む際の埋込ロジックとして、コンテンツ管理者 2 側とコンテンツ利用者 3 側との間で予め設定されたものを用いる場合は、このようなデータ構成とすることができる。

【 0 0 3 5 】

コンテンツ利用者 3 側において、複数の埋込ロジックに対応して電子透かしを復号化することが可能な場合には、コンテンツ管理者 2 が合成データ 1 2 中に埋込ロジックに関する情報を含ませて送ることが必要となる。この場合、図 3 に示すように、埋込ロジックに関する情報を付属データ部 1 7 に格納して、見出しデータ部 1 6、実データ部 1 5 とともに合成データ 1 2 を作成することが考えられる。

【 0 0 3 6 】

付属データ部 1 7 には、埋込ロジックに関する情報の他に、許諾情報が電子透かしとして見出しデータ部に埋め込まれている位置と電子透かしのサイズに関する位置情報、デジタルコンテンツの使用期限や使用回数制限などに関する使用制限情報などを格納することも可能である。また、この付属データ部 1 7 に格納される情報を暗号化することが考えられ、たとえば、許諾情報を生成した際に用いた利用者情報 1 4 で暗号化するように構成できる。

【 0 0 3 7 】

さらに、許諾情報を暗号化する際に用いた暗号鍵である利用者情報 1 4 は、見出しデータ部 1 6 に電子透かしとして埋め込むことも可能であり、付属データ部 1 7 に格納することも可能である。この場合には、コンテンツ利用者 3 がデジタルコンテンツを再生する前に、本人認証を行うことが可能となり、不正利用を防止することが可能となる。

【 0 0 3 8 】

なお、コンテンツ提供者 1 とコンテンツ管理者 2 は同一であってもよい。

〔コンテンツ管理者〕

コンテンツ管理者 2 側の概略構成を示す機能ブロック図を図 4 に示す。

【 0 0 3 9 】

このコンテンツ管理者 2 側では、運用を行うコンテンツを管理するコンテンツ管理部 2 1、所定のコンテンツ鍵を用いてデジタルコンテンツを暗号化するコンテンツ暗号化部 2 2、コンテンツ鍵を管理するコンテンツ鍵管理部 2 3、コンテンツ利用者 3 の利用者情報を取得してこれを管理する利用者情報管理部 2 4、利用者情報管理部 2 4 で管理している利用者情報情報に基づいてデジタルコンテンツの利用許諾情報を作成しこれを管理する許諾情報管理部 2 5、デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにシンボル化したシンボル情報を備える見出しデータ部を作成し、この見出しデータ部に許諾情報を電子透かしとして埋め込む見出しデータ作成部 2 6、コンテンツ鍵を用いてデジタルコンテンツを暗号化した実データ部と許諾情報付見出しデータ部とを合成する合成データ作成部 2 7などを備えている。

【 0 0 4 0 】

〔コンテンツ利用者〕

コンテンツ利用者 3 側の概略構成を示す機能ブロック図を図 5 に示す。

このコンテンツ利用者 3 側では、使用しているハードディスクドライブの識別番号、コンピュータに搭載されている CPU の識別番号、その他の利用者固有の識別情報を管理する利用者情報管理部 3 1、コンテンツ管理者 2 からの合成データを取得するための合成データ取得部 3 2、取得した合成データのうち見出しデータ部を表示するための見出しデータ表示部 3 3、許諾情報付見出しデータ部から許諾情報を分離する許諾情報抽出部 3 4、抽出した許諾情報を復号化してコンテンツ鍵を再生するコンテンツ鍵復号部 3 5、復号化されたコンテンツ鍵を用いて暗号化コンテンツを復号化するコンテンツ復号部 3 6、復号化したデジタルコンテンツを動作させるコンテンツ動作部 3 7などを備えている。

【 0 0 4 1 】

〔コンテンツ配布〕

コンテンツ管理者 2 側において、デジタルコンテンツを配布する際の手順について、図 6 に示すフローチャートに基づいて説明する。

【 0 0 4 2 】

ステップ S 1 1 では、配布を行う合成データ 1 2 中に格納するデジタルコンテンツを選択する。このデジタルコンテンツは、静止画像データ、動画画像データ、音声データ、音楽データおよびこれらを複合的に含む電子化データであり、たとえば、JPEG、TIFF、GIF、ビットマップ、その他の形式による画像データを選択でき、また、MP3、WAV、その他の形式による音声データを選択することが可能である。

【 0 0 4 3 】

ステップ S 1 2 では、選択した各デジタルコンテンツについて、その属性を視覚的または聴覚的に認識できるようにしたシンボル情報を作成する。このシンボル情報は、そのデジタルコンテンツのデータ形式に対応するアイコンを当てはめることが可能である。

【 0 0 4 4 】

たとえば、各シンボル情報はアイコンのような画像データを用いることが可能であり、たとえば、図 8 のデータテーブルに示すように、データ種別、シンボル情報、デジタルコンテンツのデータ形式に基づく拡張子をそれぞれ対応させて定義しておくことができる。

【 0 0 4 5 】

ステップ S 1 3 では、各デジタルコンテンツに対応して作成したシンボル情報が埋め込まれた見出しデータ部 1 6 を作成する。見出しデータ部 1 6 は、たとえば、画像データとして生成された各デジタルコンテンツのシンボル情報が、1 つの画像データ中に埋め込まれた構成とすることができる。また、音声データとした場合には、各デジタルコンテンツのシンボル情報が、順次連結された 1 つの音声データとすることも可能である。また、画像データ中に埋め込まれたシンボル情報が、音声データを伴うように構成することも可能である。

【 0 0 4 6 】

ステップ S 1 4 では、合成データ 1 2 中に格納される各デジタルコンテンツに権利情報の埋込処理を行う。この権利情報は、デジタルコンテンツの著作権情報や出版権情報などを示すものであり、必要に応じてデジタルコンテンツ中への埋込処理が行われる。権利情報のデジタルコンテンツへの埋込処理は、不可視また

は不可聴の電子透かしとして埋め込むことが可能であり、可視的または可聴的な電子透かしとすることも可能である。

【 0 0 4 7 】

ステップ S 1 5 では、合成データ 1 2 中に格納される各デジタルコンテンツをそれぞれ対応するコンテンツ鍵により暗号化して実データ部 1 5 を作成する。暗号化する方法は、各種暗号法を採用することができ、特に秘密鍵暗号系による暗号化を行うことが好ましい。この場合、各デジタルコンテンツに対応してコンテンツ管理者 2 側でコンテンツ鍵を自動生成し、このコンテンツ鍵を用いて暗号化された実データ部の生成を行う。デジタルコンテンツ毎に異なるコンテンツ鍵を用いるように構成することも可能であり、合成データ中の各デジタルコンテンツを共通のコンテンツ鍵を用いて暗号化するように構成することも可能である。

【 0 0 4 8 】

ステップ S 1 6 では、デジタルコンテンツを暗号化する際に用いたコンテンツ鍵の情報を含む許諾情報を生成し、この許諾情報を見出しデータ 1 6 に埋め込む。許諾情報は、デジタルコンテンツの暗号化に用いたコンテンツ鍵を、コンテンツを利用するユーザに固有の利用者情報 1 4 を用いて暗号化したものとしてすることができる。このユーザに固有の利用者情報 1 4 は、ユーザに対して予め設定されたパスワードとすることができる。また、この利用者情報 1 4 は、ユーザがデジタルコンテンツを動作させる際に使用する情報機器の識別情報とすることができる。たとえば、パソコンに搭載されている CPU のシリアルナンバー、CD-ROM、DVD、MO、FD、HD などドライブのシリアルナンバーが採用され得る。この場合、ユーザのパスワードまたは使用する情報機器の識別情報をコンテンツ管理者 2 側で登録しておき、この登録されている利用者情報 1 4 に基づいてコンテンツ鍵を暗号化するように構成できる。

【 0 0 4 9 】

さらに、ユーザに固有の利用者情報 1 4 として、ユーザの生体情報を用いることが可能である。たとえば、ユーザの指紋情報、網膜情報、虹彩情報、声紋情報などを予めコンテンツ管理者 2 側に登録しておき、各生体情報に基づいてコンテンツ鍵を暗号化するように構成できる。たとえば、指紋情報を用いてコンテンツ

鍵を暗号化する場合、予めユーザからコンテンツ管理者 2 側に利用者本人の指紋画像を登録してもらう。コンテンツ管理者 2 側では、登録されているユーザの指紋画像を分析して、指紋画像のうち端点・分岐点などのマニューシャと呼ばれる特徴点を抽出し、この特徴点情報によりコンテンツ鍵を暗号化する。

【0050】

ステップ 16 では、コンテンツ鍵を利用者情報 14 により暗号化した許諾情報 13 を見出しデータ部 16 に電子透かしとして埋め込む。この見出しデータ 16 への許諾情報 13 の埋め込みは、不可視または不可聴の電子透かしとして埋め込む構成とすることができ、見出しデータ 16 の特定の周波数帯域に許諾情報 13 を挿入する、データの一部を間引きしてここに許諾情報を挿入する、その他の方法が考えられる。

【0051】

ステップ S17 では、見出しデータ部 16 と実データ部 15 とを合成して合成データ 12 を作成する。見出しデータ部 16 に許諾情報 13 を埋め込む際の埋め込みロジックを格納する付属データ部 17 を必要とする場合には、見出しデータ部 16、実データ部 15 とともに付属データ部 17 を合成して合成データ 12 (図 3 参照) を作成する。

【0052】

このようにして作成された合成データ 12 は、CD-ROM、DVD、光磁気ディスク (MO)、MD、フロッピーディスク、その他の記録媒体に記録されてユーザに送られるか、あるいはインターネットを通じて直接ユーザのパソコンなどの情報機器に配信され、ハードディスク上に格納される。

【0053】

〔コンテンツ利用〕

配布された合成データ 12 をコンテンツ利用者 3 側で利用する場合について、図 7 のフローチャートに基づいて説明する。

【0054】

ステップ S21 では、合成データ 12 から実データ部 15 と見出しデータ 16 とを分離する。付属データ部 17 がある場合には同時にこの付属データ部 17 も

分離する。

【 0 0 5 5 】

ステップ S 2 2 では、見出しデータ部 1 6 に電子透かしとして埋め込まれている許諾情報 1 3 を取り出して、この許諾情報 1 3 からコンテンツ鍵を復号化する。許諾情報 1 3 は見出しデータ部 1 6 に所定の埋め込みロジックにより電子透かしとして埋め込まれており、コンテンツ管理者 2 とコンテンツ利用者 3 との間で予め決めた埋め込みロジックを使って、許諾情報 1 3 を取り出すことが可能である。

【 0 0 5 6 】

付属データ部 1 7 に、電子透かしの埋め込みロジックが格納されている場合には、この付属データ部 1 7 から埋め込みロジックの情報を取り出して、これに基づいて許諾情報 1 3 を取り出すように構成する。電子透かしが埋め込まれている位置やサイズに関する位置情報が付属データ部 1 7 に格納されている場合も、この位置情報を付属データ部 1 7 から取り出してこれを利用して許諾情報 1 3 を取り出す。

【 0 0 5 7 】

許諾情報 1 3 は、利用者情報 1 4 に基づく暗号鍵によって暗号化されたものであり、利用者情報 1 4 を用いて復号化が可能となる。利用者情報 1 4 がパスワードである場合には、ユーザによるパスワードの入力を受け付けてこの入力パスワードを用いて許諾情報 1 3 を復号化する。また、CPU のシリアルナンバーやメディアドライブのシリアルナンバーなどでなる情報機器の識別情報により暗号化されている場合には、現在使用している情報機器の識別情報を取得して、これに基づいて許諾情報 1 3 を復号化する。さらに、ユーザの生体情報で暗号化されている場合には、ユーザの生体情報の入力を受け付けて、これを端点・分岐点などによる特徴点情報に解析し、この特徴点情報により復号化するように構成できる。

【 0 0 5 8 】

ユーザから受け付けたパスワード、ユーザが現在使用している情報機器の識別情報、ユーザから受け付けた生体情報に基づく特徴点情報などが正常であれば、許諾情報 1 3 から正当なコンテンツ鍵が復元されることとなる。

【 0 0 5 9 】

ステップ S 2 3 では、復元されたコンテンツ鍵を用いて実データ部 1 5 を復号化してデジタルコンテンツの復元を行う。復元されたデジタルコンテンツは、コンテンツ利用者 3 側のハードディスクやその他の記録媒体上で展開されて格納される。

【 0 0 6 0 】

ステップ S 2 4 では、見出しデータ部 1 6 に記録されているシンボル情報に基づいて、このシンボル情報に定義付けされているファイル拡張子情報を抽出して、復元されたデジタルコンテンツと関連付ける。

【 0 0 6 1 】

ステップ S 2 5 では、ユーザの指示に基づいて、ファイル拡張子情報に関連するアプリケーションを起動し、デジタルコンテンツの利用を行う。復元されたデジタルコンテンツが実行形式のファイルである場合には、ユーザによるアプリケーションの起動を待たずに、ファイルの指定があれば自己起動するように構成できる。

【 0 0 6 2 】

〔生体情報による認証方法〕

デジタルコンテンツを利用しようとしているユーザが、正当な利用者であるか否かの認証を、ユーザの生体情報を用いて行うことが可能である。生体情報としては、前述のように、指紋情報、網膜情報、虹彩情報、声紋情報などが考えられる。ここでは、指紋情報を用いて認証を行う場合について、図 9、図 1 0 に基づいて説明する。

【 0 0 6 3 】

ユーザの指紋情報に基づいて本人認証を行う場合には、予めユーザからコンテンツ管理者 2 側に利用者本人の指紋画像を登録してもらう。ステップ S 3 1 では、登録されているユーザの指紋画像に基づいて、検査対象となる指紋との照合を行うテンプレート情報を作成する。

【 0 0 6 4 】

指紋画像の端点・分岐点などのマニューシャと呼ばれる特徴点情報による照合

を行う場合には、登録されている指紋画像から特徴点情報を抽出してこれをテンプレート情報として登録する。

【 0 0 6 5 】

また、登録されているユーザの指紋画像を細線化画像とし、検査対象となる指紋の二値化画像とのパターンマッチングを行う方法を用いる場合には、登録されているユーザの指紋画像から細線化画像を作成し、これをテンプレート情報とする。

【 0 0 6 6 】

ステップ S 3 2 では、登録されているユーザの指紋画像から作成したテンプレート情報を見出しデータ部 1 6 または付属データ部 1 7 に記録する。見出しデータ部 1 6 にテンプレート情報を記録する場合には、不可視な電子透かしとして埋め込むように構成できる。また、付属データ部 1 7 を有するデータ構造である場合には、この付属データ部 1 7 にテンプレート情報を格納するように構成できる。

【 0 0 6 7 】

コンテンツ利用者 3 側では、図 1 0 に示すフローチャートに基づいて本人認証動作を行う。

ステップ S 4 1 では、コンテンツ利用者 3 側に設置される指紋読取装置によりユーザの指紋を読み取り、その指紋画像から検査対象となる指紋情報を取得する。前述したように、指紋の特徴点に基づいて照合を行う場合には、読み取った指紋画像からその端点・分岐点などに基づく特徴点情報を生成する。また、細線化画像とのパターンマッチングを行う場合には、読み取った指紋画像から二値化画像を生成する。

【 0 0 6 8 】

ステップ S 4 2 では、見出しデータ部 1 6 または付属データ部 1 7 に記録されているテンプレート情報を取り出す。見出しデータ部 1 6 にテンプレート情報が電子透かしとして記録されている場合には、所定の埋め込みロジックにより見出しデータ部 1 6 からテンプレート情報を取り出すこととなる。

【 0 0 6 9 】

ステップ S 4 3 では、検査対象となる指紋情報とテンプレート情報とを照合して本人認証を行う。特徴点情報に基づいて照合を行う場合には、検査対象となる指紋画像から得た特徴点情報と、登録されているユーザの指紋から得た特徴点情報であるテンプレートが比較され、その比較結果に基づいて本人認証が行われる。また、細線化画像による照合を行う場合には、検査対象となる指紋画像の二値化情報と、登録されているユーザの指紋から得た細線化画像とをパターンマッチングし、その結果に基づいて本人認証が行われる。

【 0 0 7 0 】

〔コンテンツ利用情報〕

利用者情報 1 4 などのユーザに関する情報をデジタルコンテンツ内に埋め込むことで、利用状況をデジタルコンテンツ内に残すことが可能である。たとえば、配布を行う合成データ 1 2 中のデジタルコンテンツに配布先であるユーザの利用者情報 1 4 を埋め込むことで、最初に配布を行ったユーザの情報を残すことが可能となる。また、デジタルコンテンツの利用時にそのユーザの利用者情報 1 4 を取得し、これをデジタルコンテンツ中に埋め込むように構成すれば、利用者の履歴を残すことができる。

【 0 0 7 1 】

デジタルコンテンツ内に利用するユーザの指紋情報を埋め込む場合について、図 1 1 のフローチャートに基づいて説明する。

ステップ S 5 1 では、デジタルコンテンツを利用しようとするユーザの指紋画像情報を生成する。

【 0 0 7 2 】

ステップ S 5 2 では、合成データのデジタルコンテンツ内にユーザの指紋画像情報を埋め込む。

たとえば、コンテンツ管理者 2 側において、配布する合成データ 1 2 中に含まれるデジタルコンテンツに、予め登録されている配布先のユーザの指紋画像情報を、不可視な電子透かしとして埋め込むことが考えられる。この場合、最初に配布を行ったユーザの指紋画像情報がデジタルコンテンツ内に埋め込まれており、不正にコピーされた場合であってもその出所を判別することが可能となる。

【 0 0 7 3 】

また、デジタルコンテンツを利用しようとする際に、ユーザの指紋画像情報を取得し、これをデジタルコンテンツ内に埋め込むように構成することも可能である。この場合も、利用しようとするユーザの指紋画像情報を不可視な電子透かしとしてデジタルコンテンツ内に埋め込むように構成できる。この場合、不正に利用しようとした場合であっても、デジタルコンテンツに利用者の履歴情報が残ることとなり、このデータが不正に流出した経路を知ることができる。

【 0 0 7 4 】

〔電子透かし埋め込みロジック〕

前述したように、見出しデータ部 1 6 に許諾情報 1 3 を不可視な電子透かしとして埋め込む場合に、許諾情報 1 3 を埋め込む際に用いた埋め込みロジックの情報を合成データ 1 2 内に持たせることができる。見出しデータ部 1 6 には、許諾情報 1 3 の他にユーザの生体情報、著作権や版權などに関する権利情報などを電子透かしとして埋め込むことが考えられ、またデジタルコンテンツ内にも、ユーザの生体情報、著作権や版權などに関する権利情報、利用期限や利用回数制限などに関する利用情報などを埋め込むことが考えられる。見出しデータ部 1 6 と実データ部 1 5 に含まれる電子透かしの埋め込みロジックの種別やバージョン情報をそれぞれ付属データ部 1 7 に格納しておくことで、コンテンツ利用者 3 側での利用が容易となる。この動作について、図 1 2 および図 1 3 のフローチャートに基づいて説明する。

【 0 0 7 5 】

ステップ S 6 1 では、配布する合成データ 1 2 の見出しデータ部 1 6 および実データ部 1 5 のそれぞれに含まれる電子透かしの埋め込みロジックの種別データとバージョン情報を付属データ部 1 7 に格納する。

【 0 0 7 6 】

たとえば、見出しデータ部 1 6 および実データ部 1 5 で使用される埋め込みロジックを、図 1 4 のテーブルのように定義することができる。ここでは、見出しデータ部 1 6 で使用される埋め込みロジックの種別とバージョン情報および実データ部 1 5 で使用される埋め込みロジックの種別とバージョン情報を順に並べて

4 桁の数値とし、これに基づいて埋め込みロジックを定義している。

【 0 0 7 7 】

ステップ S 6 2 では、付属データ部 1 7 に設定された埋め込みロジックにしたがって、見出しデータ部 1 6 および実データ部 1 5 にそれぞれ電子透かしの埋め込み処理を実行する。

【 0 0 7 8 】

コンテンツ利用者 3 側において、配布された合成データ 1 2 から電子透かしのデータを取り出す場合には、図 1 3 のフローチャートに基づいて動作する。

ステップ S 7 1 では、合成データ 1 2 中の付属データ部 1 7 から埋め込みロジックの情報を取得する。

【 0 0 7 9 】

ステップ S 7 2 では、取得した埋め込みロジックの情報に基づいて、見出しデータ部 1 6 および実データ部 1 5 に埋め込まれた電子透かしを取り出す。取得した埋め込みロジックの情報は、前述したように、見出しデータ部 1 6 に対する埋め込みロジックの種別とバージョン情報および実データ部 1 5 に対する埋め込みロジックの種別とバージョン情報で構成されており、これに基づいて各電子透かしの情報を取り出すことが可能となる。

【 0 0 8 0 】

〔実データ部のハッシュ値〕

デジタルコンテンツの内容の改竄やデータの置き換え、通信中のエラーなどを検出するために、実データ部 1 5 のハッシュ値を生成し、これを合成データ 1 2 中に記録しておく構成とすることができる。ハッシュ値は、ハッシュ関数を用いて求められる固定長の疑似乱数であり、このハッシュ値から原文を再現することができないように、不可逆な一方方向関数により生成される。

【 0 0 8 1 】

このような見出しデータ部 1 5 のハッシュ値を見出しデータ部 1 6 に埋め込む場合について、図 1 5 および図 1 6 のフローチャートに基づいて説明する。

ステップ S 8 1 では、実データ部 1 5 のデータを特定のハッシュ関数に入力しハッシュ値を生成する。ハッシュ値を求める実データ部としては、暗号化前のデ

デジタルコンテンツのデータとすることも可能であり、コンテンツ鍵による暗号化された実データ部とすることも可能である。また、ハッシュ関数は、SHA-1やMD5、その他のものを用いることが可能である。

【 0 0 8 2 】

ステップ S 8 2 では、生成された実データ部 1 5 のハッシュ値を見出しデータ部 1 6 に不可視な電子透かしとして埋め込む。電子透かしの埋め込みロジックは、前述したような埋め込みロジック種別およびバージョン情報で定義されたものを用いることができる。

【 0 0 8 3 】

合成データ 1 2 に含まれる実データ部 1 5 のハッシュ値を求め、見出しデータ部 1 6 に埋め込まれたハッシュ値と比較することによって、データの置き換えなどの不正があったことを検証することができる。このときの動作を図 1 6 のフローチャートに基づいて説明する。

【 0 0 8 4 】

ステップ S 9 1 では、合成データ 1 2 中に含まれる実データ部 1 5 のデータを特定のハッシュ関数に入力し、ハッシュ値を求める。ここでは、見出しデータ 1 6 中に電子透かしとして埋め込まれたハッシュ値と同じハッシュ関数を用いることが必要である。

【 0 0 8 5 】

ステップ S 9 2 では、合成データ 1 2 の見出しデータ部 1 6 に埋め込まれているハッシュ値を抽出する。ハッシュ値は、前述の埋め込みロジックに基づいて電子透かしとして見出しデータ部 1 6 に埋め込まれており、この埋め込みロジックに基づいて抽出することで検証用のハッシュ値を取得することができる。

【 0 0 8 6 】

ステップ S 9 3 では、ハッシュ関数により生成した実データ部 1 5 のハッシュ値と、見出しデータ部 1 6 から抽出した検証用のハッシュ値を比較して一致するか否かの検証を行う。

【 0 0 8 7 】

このように、見出しデータ部 1 6 に実データ部 1 5 のハッシュ値を埋め込むこ

とにより、合成データ 1 2 に含まれるデジタルコンテンツが改竄されたことや不正にデータの置き換えがあったことを認識することが可能となる。

【 0 0 8 8 】

〔サーバの記録場所情報〕

配布する合成データ 1 2 中に含まれるデジタルコンテンツを管理しているサーバの記録場所情報を合成データ 1 2 中に含ませることができる。この場合の動作について図 1 7 および図 1 8 のフローチャートに基づいて説明する。

【 0 0 8 9 】

ステップ S 1 0 1 では、配布するデジタルコンテンツを管理するサーバの格納情報を取得する。この場合、サーバ内のデジタルコンテンツが格納されている場所を示す URL などを格納情報として取得する。

【 0 0 9 0 】

ステップ S 1 0 2 では、見出しデータ部 1 6 に不可視な電子透かしとして格納情報を埋め込む。この場合も、前述と同様にして設定された埋め込みロジックを用いて電子透かしの埋め込みが行うことができる。

【 0 0 9 1 】

ステップ S 1 0 3 では、見出しデータ部 1 6 に埋め込んだものと同じ格納情報を付属データ部 1 5 に格納する。

配布されたデジタルコンテンツを管理するサーバの URL と、見出しデータ部 1 6 に埋め込まれた格納情報および付属データ部 1 5 に格納されている格納情報とを検証すれば、デジタルコンテンツが正常に利用されていることを確認することができる。

【 0 0 9 2 】

ステップ S 1 1 1 では、デジタルコンテンツを管理するサーバの記録場所情報を取得する。

ステップ S 1 1 2 では、見出しデータ部 1 6 に埋め込まれている格納情報を抽出する。この場合、前述したような見出しデータ部 1 6 に対応する埋め込みロジックを用いて格納情報を抽出する。

【 0 0 9 3 】

ステップ S 1 1 3 では、付属データ部 1 7 に格納されている格納情報を抽出する。

ステップ S 1 1 4 では、サーバの格納情報、見出しデータ部 1 6 から抽出した格納情報および付属データ部 1 7 から抽出した格納情報を比較して、同じ値であるか否かを検証する。

【 0 0 9 4 】

このように構成した場合、見出しデータ部 1 6、実データ部 1 5 および付属データ部 1 7 を分離して不正利用しても、各格納情報を比較して検証することで不正利用を発見することが可能である。また、見出しデータ部 1 6 に埋め込まれた格納情報と、付属データ部 1 7 に格納された格納情報とを同じように置き換えたとしても、デジタルコンテンツを管理しているサーバの格納情報と比較して検証しているため、不正利用を発見することが可能となる。

【 0 0 9 5 】

〔セキュリティ要求と画質要求〕

画像データであるデジタルコンテンツ内に電子透かしを埋め込む場合には、ある程度画質が劣化することが問題となる。したがって、高画質が求められるようなデジタルコンテンツについては、可視的な電子透かしを埋め込むことが考えられる。また、セキュリティ要求が低いデジタルコンテンツについては、暗号化する必要もない場合がある。このような画質要求とセキュリティ要求とに基づいて、電子透かしの形態と暗号化の有無を各デジタルコンテンツについて設定することが可能である。

【 0 0 9 6 】

デジタルコンテンツを合成データ 1 2 内のデータとして取り込む際に、画質要求とセキュリティ要求に基づいて実データ部 1 5 を作成する方法を図 1 9 のフローチャートに基づいて説明する。

【 0 0 9 7 】

ステップ S 1 2 1 では、画質要求情報とセキュリティ要求情報とを入力する。たとえば、図 2 0 に示すように、画質要求情報およびセキュリティ要求情報を、それぞれ“LOW”および“HIGH”とし、この組み合わせにしたがって、電子透かしの

形態および暗号化の有無を設定するように構成できる。

【0098】

ステップS122では、入力された画質要求情報とセキュリティ要求情報に基づいて、図20のテーブルを参照し、電子透かしの形態と暗号化の有無を決定して実データ部15の生成を実行する。

【0099】

この場合、画質要求が高いデジタルコンテンツについては、不可視な電子透かしを用いずに画質の劣化を防止することが可能となる。著作権情報や版權に関する情報などについては、可視的な透かしとして埋め込むように構成しているため、不正な利用を防止することが可能となる。

【0100】

また、セキュリティ要求の高いデジタルコンテンツについてはコンテンツ鍵を用いた暗号化を行っており、セキュリティ効果を維持することができ、セキュリティ要求の低いデジタルコンテンツについては暗号化を省略することで、配布時における合成データ作成の時間の短縮および利用時における起動時間の短縮を図ることが可能となる。

【0101】

〔他の実施形態〕

(A) コンテンツ管理者2または他の特定の連絡先情報を見出しデータ部16内に電子透かしと埋め込んだ構成とすることができる。この場合、ユーザ側で合成データ12内のデジタルコンテンツを利用する際に、見出しデータ部16から抽出した連絡先に回線接続を行い、コンテンツ情報を送出するように構成できる。

【0102】

このことで、配布されたデジタルコンテンツの利用状況をコンテンツ管理者2側で監視することができ、不正利用を防止することが可能となる。

(B) 合成データ12中に含まれるデジタルコンテンツ11の内容を代表するようなサンプルデータを抽出し、このサンプルデータを見出しデータ部とすることが可能である。

【0103】

たとえば、デジタルコンテンツ11が画像データを含む構成である場合に、このうち代表的な画像データを抽出し、この画像データに前述したような許諾情報13を埋め込んで許諾情報付見出しデータ部16を作成することが可能である。

【0104】

デジタルコンテンツ11が音楽データや音声データである場合には、その一部をサンプリングして、デジタルコンテンツの内容がわかるように構成することができる。

【0105】

さらに、各デジタルコンテンツのタイトルや要約を読み上げた音声データを用いることも可能であり、この場合は、音楽データであるデジタルコンテンツの一部をサンプリングして見出しデータ部とする場合と同様に取り扱うことが可能である。

〔付記項〕

(付記1)

配布を行うデジタルコンテンツを暗号化して実データ部を作成し、前記デジタルコンテンツの属性を視覚的または聴覚的に認識できるようにシンボル化したシンボル情報を備える見出しデータ部を作成し、前記デジタルコンテンツの暗号化の際に暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を電子透かしとして前記見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成してこれを配布するデータ運用方法。

(付記2)

前記見出しデータ部は、複数のデジタルコンテンツにそれぞれ対応してその内容を視覚的に認識できるようにシンボル化された1つ以上の画像シンボルデータを、1つの画像データ内に合成してなる、付記1に記載のデータ運用方法。

(付記3)

配布を行うデジタルコンテンツを暗号化して実データ部を作成し、前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした

見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記デジタルコンテンツの利用制限を行うための利用制限情報を暗号化した付属データ部を作成し、前記実データ部と前記許諾情報付見出しデータ部とを合成する際に前記付属データ部を同時に合成して合成データを作成してこれを配布するデータ運用方法。

(付記 4)

前記利用制限情報は、前記許諾情報を前記見出しデータ部に電子透かしとして埋め込む際の埋込ロジックである、付記 3 に記載のデータ運用方法。

(付記 5)

前記利用制限情報は、前記デジタルコンテンツを利用可能な利用期限または利用回数に基づく、付記 3 に記載のデータ運用方法。

(付記 6)

前記利用制限情報は、前記デジタルコンテンツの利用者の個人情報を暗号鍵として暗号化されている、付記 3 ～ 5 のいずれかに記載のデータ運用方法。

(付記 7)

前記利用制限情報を暗号化する際の暗号鍵は、前記利用者によって予め設定されたパスワードである、付記 6 に記載のデータ運用方法。

(付記 8)

前記利用制限情報を暗号化する際の暗号鍵は、前記合成データが記録される記録媒体に固有の識別情報である、付記 6 に記載のデータ運用方法。

(付記 9)

前記利用制限情報を暗号化する際の暗号鍵は、前記利用者の生体情報である、付記 6 に記載のデータ運用方法。

(付記 1 0)

配布を行うデジタルコンテンツを暗号化した実データ部と、
前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした

見出しデータ部に、前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部と、

前記デジタルコンテンツの利用制限を行うための利用制限情報を暗号化した付属データ部と、

を合成して配布される合成データから付属データ部を分離し、前記付属データ部を復号化して利用制限情報を取り出し、前記利用制限情報に基づいて前記許諾情報付見出しデータ部に埋め込まれた許諾情報を取り出し、前記許諾情報から前記デジタルコンテンツを復号化するためのコンテンツ鍵を取得し、このコンテンツ鍵を用いて前記実データ部を元のデジタルコンテンツに復号化して利用者に利用させるデータ運用方法。

(付記 1 1)

配布を行うデジタルコンテンツを暗号化して実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部からハッシュ関数を用いて生成されたハッシュ値を、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ後、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成してこの合成データを配布することを特徴とするデータ運用方法。

(付記 1 2)

配布を行うデジタルコンテンツを暗号化して実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報と、記録される記録媒体に固有の識別情報とを視覚的または聴覚的に認識不能な電子透かしとして前記見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成して、この合成データを配布することを特徴とするデータ運用方法。

(付記 1 3)

配布を行うデジタルコンテンツを暗号化して実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報と、前記デジタルコンテンツを再生するための情報機器に特定の動作をさせる制御コードとを視覚的または聴覚的に認識不能な電子透かしとして前記見出しデータ部に埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成して、この合成データを配布することを特徴とするデータ運用方法。

(付記 1 4)

配布を行うデジタルコンテンツを暗号化した実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部をデジタルコンテンツに復号化する際に、所定の連絡先に回線接続して、復号化を行うデジタルコンテンツのコンテンツ情報を送出するために、前記デジタルコンテンツのコンテンツ情報と、前記所定の連絡先情報とを、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ後、前記実データ部と前記許諾情報付見出しデータ部とを合成した合成データを作成し、この合成データを配布することを特徴とするデータ運用方法。

(付記 1 5)

配布を行うデジタルコンテンツを暗号化した実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号

化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部と前記許諾情報付見出しデータ部を合成した合成データを作成する際に、前記デジタルコンテンツを登録しているサーバの記録場所情報を、前記合成データ中に保持させ、この合成データを配布することを特徴とするデータ運用方法。

(付記 1 6)

前記デジタルコンテンツを登録しているサーバの記録場所情報を、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込むことを特徴とする、付記 1 5 に記載のデータ運用方法。

(付記 1 7)

配布を行うデジタルコンテンツを暗号化した実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部と前記許諾情報付見出しデータ部を合成して合成データを作成する際に、前記デジタルコンテンツの利用者の生体情報に基づいて生成された生体テンプレート情報を、前記合成データ中に保持させ、この合成データを配布することを特徴とするデータ運用方法。

(付記 1 8)

前記生体テンプレート情報を、前記見出しデータ部に視覚的または聴覚的に認識不能な電子透かしとして埋め込むことを特徴とする、付記 1 7 に記載のデータ運用方法。

(付記 1 9)

配布を行うデジタルコンテンツを暗号化した実データ部を作成し、

前記デジタルコンテンツの内容を視覚的または聴覚的に認識できるようにした

見出しデータ部を作成し、前記見出しデータ部に前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を視覚的または聴覚的に認識不能な電子透かしとして埋め込んだ許諾情報付見出しデータ部を作成し、

前記実データ部と前記許諾情報付見出しデータ部を合成して合成データを作成し、この合成データを配布するデータ運用方法であって、

前記デジタルコンテンツの著作権情報や版權情報を、前記デジタルコンテンツ中に電子透かしとして埋め込むことを特徴とするデータ運用方法

。

(付記 2 0)

前記デジタルコンテンツに要求されるデータ品質レベルとセキュリティレベルとに基づいて、前記デジタルコンテンツ中に埋め込む電子透かしの形態と暗号化レベルを決定することを特徴とする、付記 1 9 に記載のデータ運用方法。

(付記 2 1)

前記デジタルコンテンツ中への電子透かしの埋め込み方式と、前記見出しデータ部への電子透かしの埋め込み方式が、異なることを特徴とする、付記 1 9 または 2 0 に記載のデータ運用方法。

【 0 1 0 6 】

【発明の効果】

本発明では、デジタルコンテンツを暗号化して配布を行う際に、添付されている見出しデータ部のシンボル情報によりその内容を認識することが容易である。したがって、配布されるデジタルコンテンツのセキュリティを高く維持することが可能であるとともに、復号化する前にどのようなデジタルコンテンツが含まれているかを確認することが可能となる。

【 0 1 0 7 】

また、デジタルコンテンツを暗号化する際に用いたコンテンツ鍵の情報を、含む許諾情報を見出しデータ部に電子透かしとして埋め込んだため、コンテンツ鍵を別途管理する必要がなく、コンテンツ鍵を紛失して再発行を受けるような手間を省くことが可能となる。このコンテンツ鍵は、ユーザの指紋情報やパスワード

ド、使用している情報機器の識別情報などを用いて暗号化することによって、正当なユーザにのみ復号化することが可能となり、不正使用を防止することができる。

【図面の簡単な説明】

【図 1】

本発明の概略構成を示すブロック図。

【図 2】

データ構造の一例を示す説明図。

【図 3】

データ構造の他の例を示す説明図。

【図 4】

コンテンツ管理者の制御ブロック図。

【図 5】

コンテンツ利用者の制御ブロック図。

【図 6】

制御の概略を示すフローチャート。

【図 7】

制御の概略を示すフローチャート。

【図 8】

シンボル情報とその種別および拡張子の対応を示すテーブル説明図。

【図 9】

認証用の指紋情報を合成データ中に記録する際の制御フローチャート。

【図 1 0】

指紋情報により本人認証を行う際の制御フローチャート。

【図 1 1】

実データ部への指紋情報を埋め込む際の制御フローチャート。

【図 1 2】

電子透かし埋め込みロジックに関する情報を合成データ中に含ませる際の制御フローチャート。

【図 1 3】

合成データ中の記録された電子透かし埋め込みロジックを用いて情報を取り出す際の制御フローチャート。

【図 1 4】

電子透かし埋め込みロジックに関する情報の一例を示すテーブル説明図。

【図 1 5】

実データ部のハッシュ値を見出しデータに埋め込む際の制御フローチャート。

【図 1 6】

実データ部のハッシュ値によりデータ中の不正の有無を検証する際の制御フローチャート。

【図 1 7】

デジタルコンテンツの管理サーバの記録場所に関する情報を合成データ中に記録する際の制御フローチャート。

【図 1 8】

デジタルコンテンツの管理サーバの記録場所に関する情報を用いて不正の有無を検証する際の制御フローチャート。

【図 1 9】

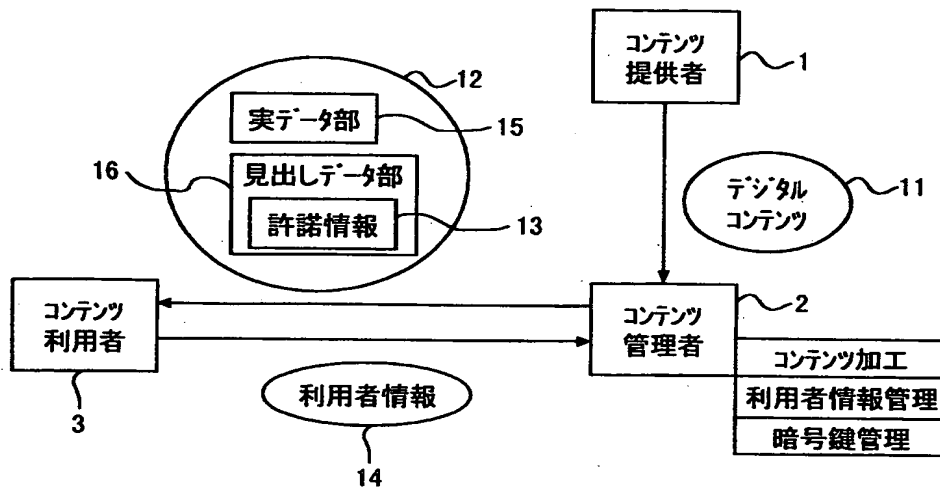
画質要求情報とセキュリティ要求情報に基づいて実データ部の生成方法を決定する際の制御フローチャート。

【図 2 0】

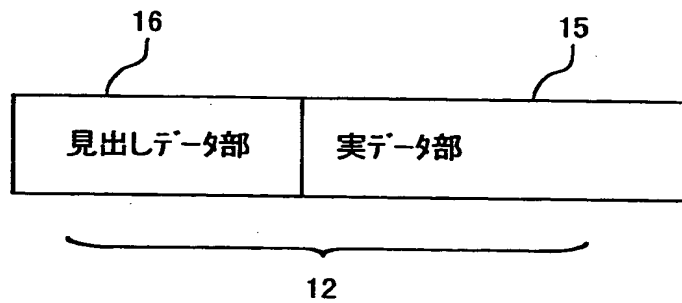
画質要求情報とセキュリティ要求情報に基づいて実データ部の生成方法を決定する際に用いるテーブルの説明図。

【書類名】 図面

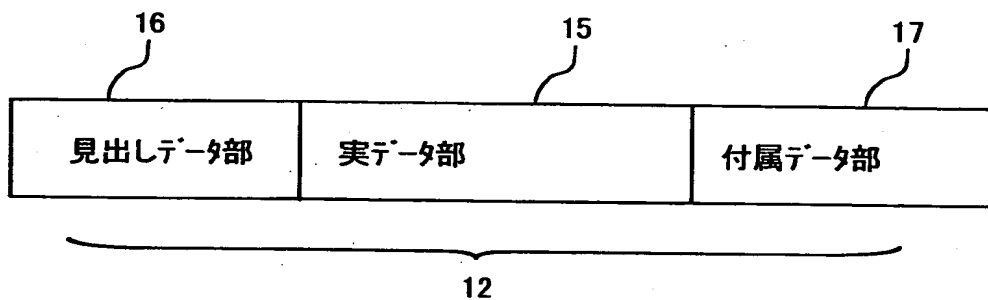
【図 1】



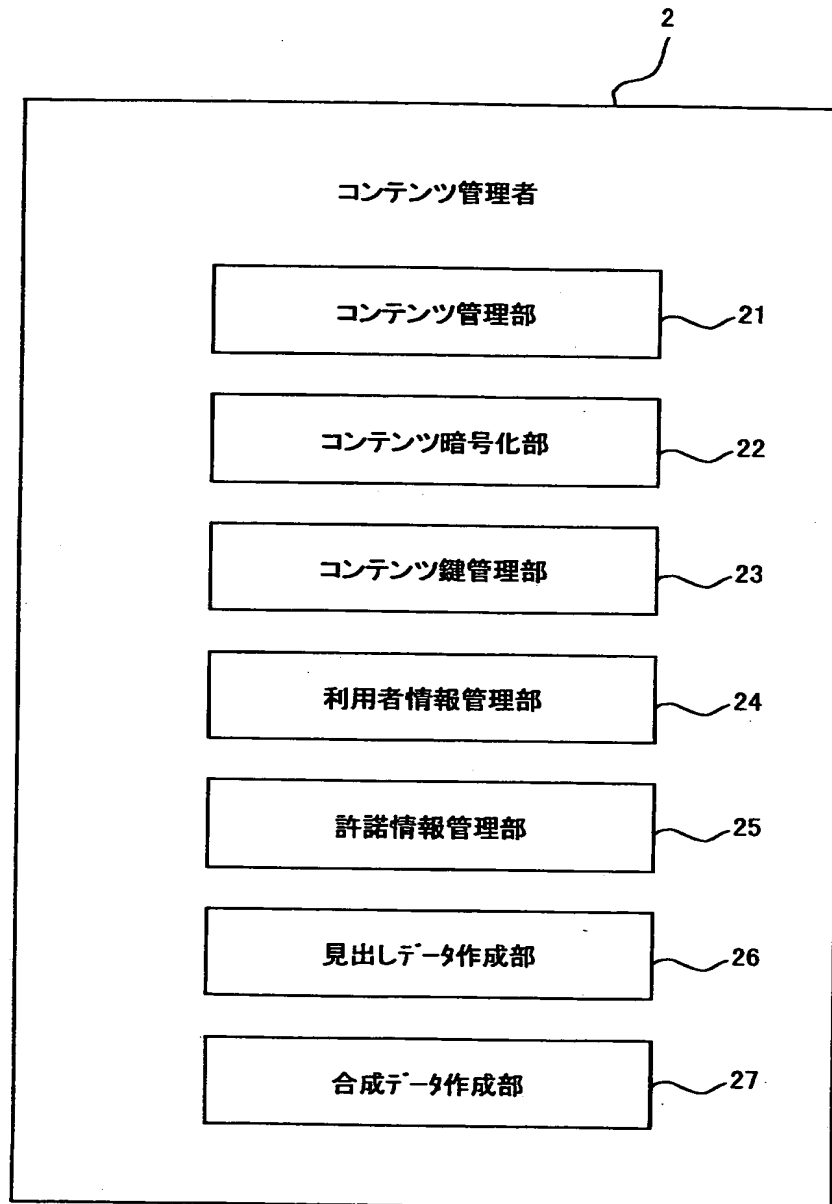
【図 2】



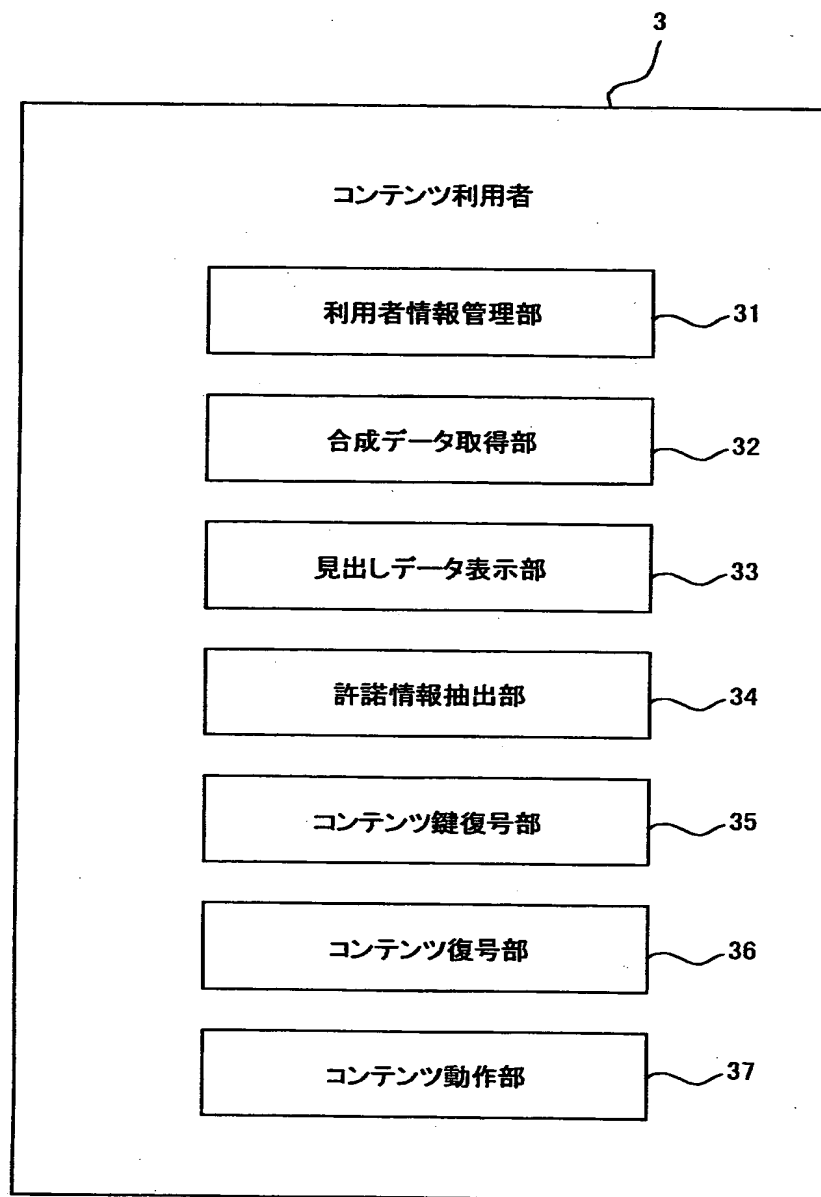
【図 3】



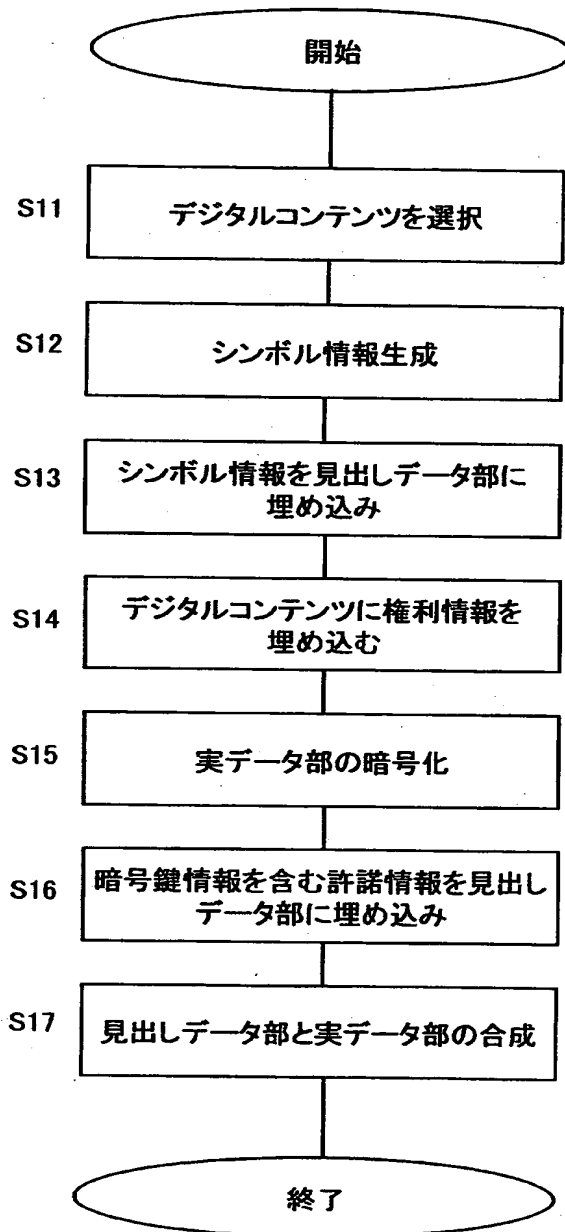
【図 4】



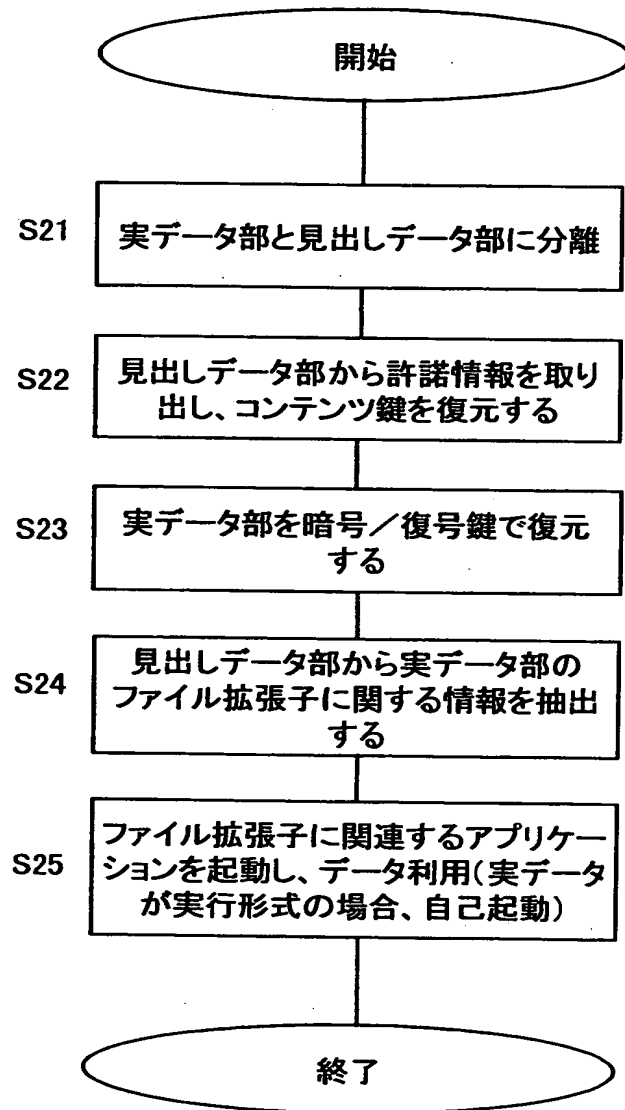
【図 5】



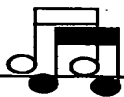


【図 6】



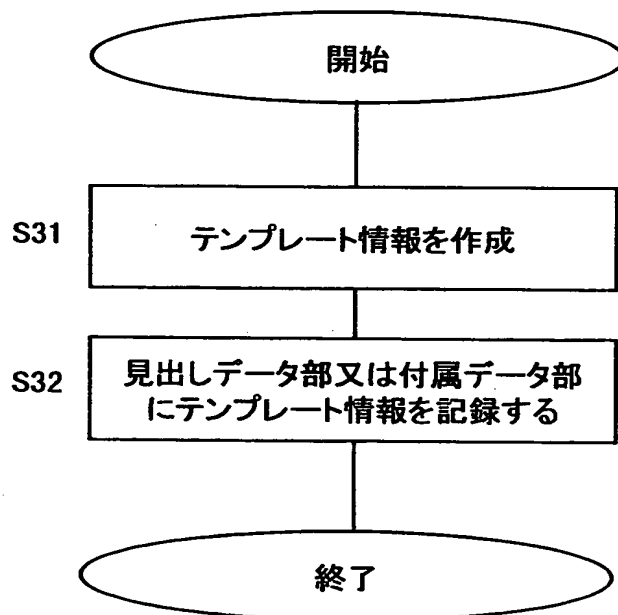
【図 7】



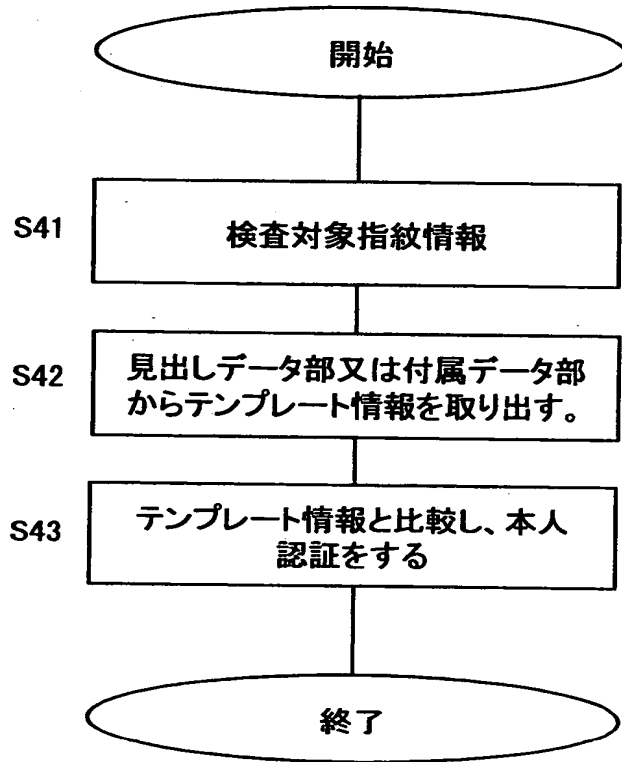
【図 8】

データ種	シンボル情報	拡張子
音楽		mp3
画像		jpg
書籍		lit

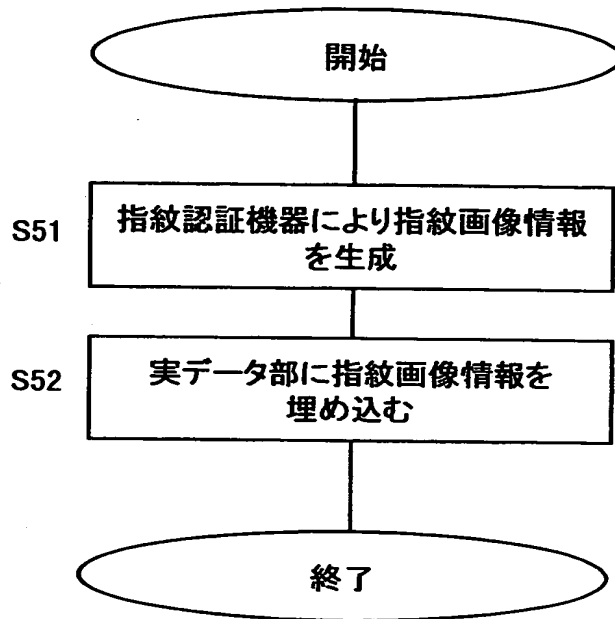
【図 9】



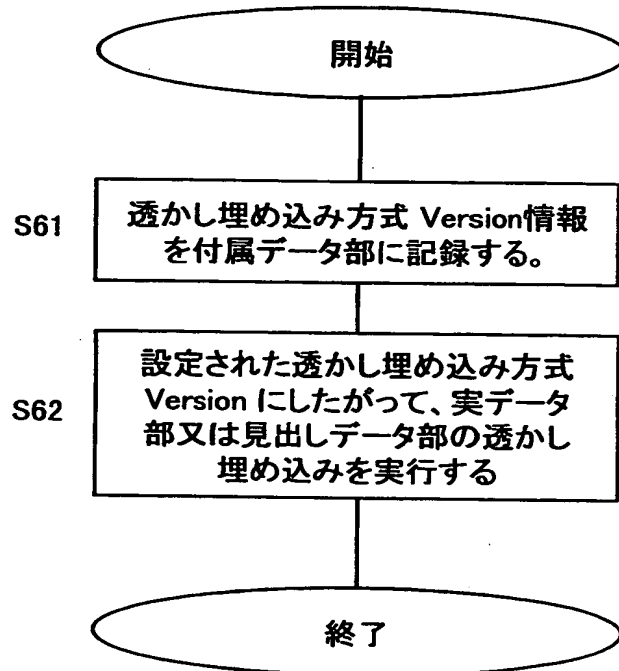
【図 1 0】



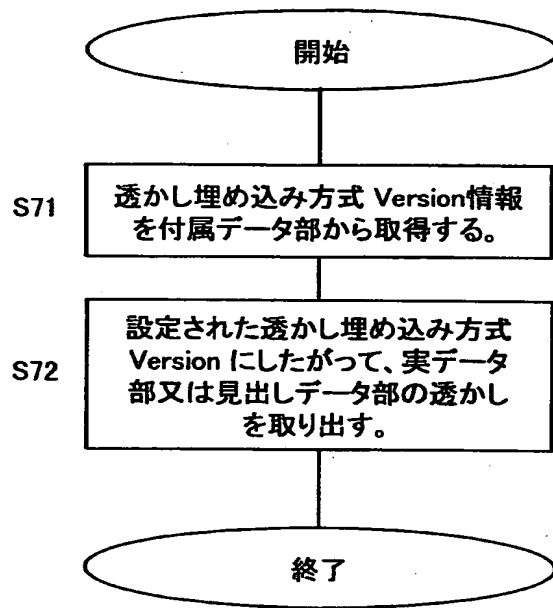
【図 1 1】



【図 1 2】



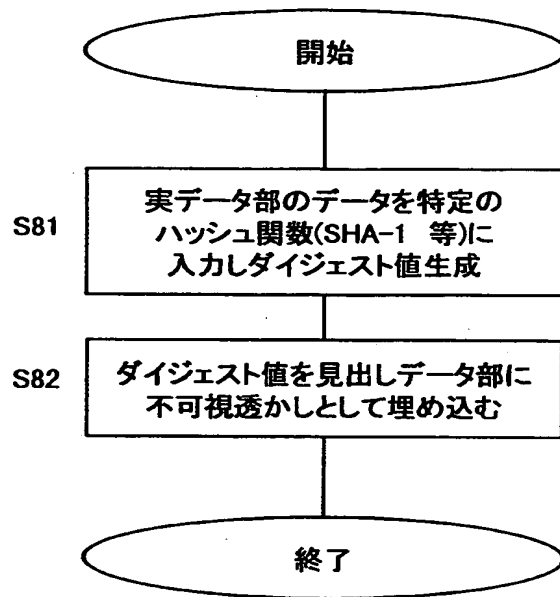
【図 1 3】



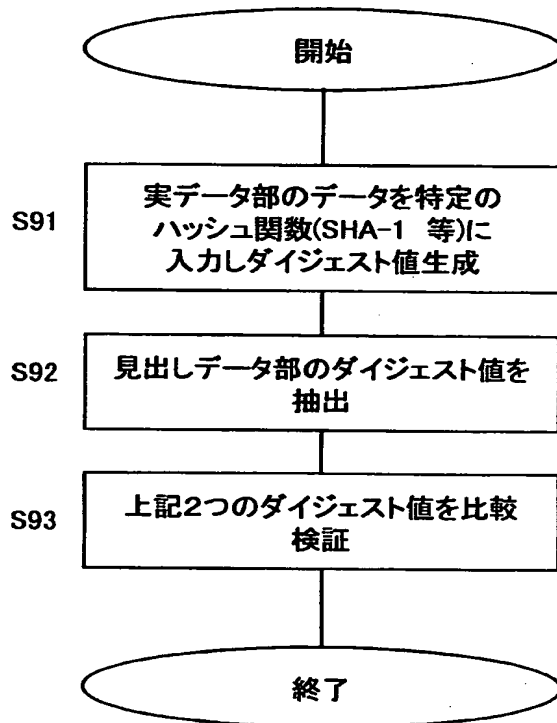
【図 1 4】

透かし埋め込み種別	見出しデータ部	実データ部
1111	Type1-Version1	Type1-Version1
2111	Type2-Version1	Type1-Version1
1100	Type1-Version1	_____

【図 1 5】



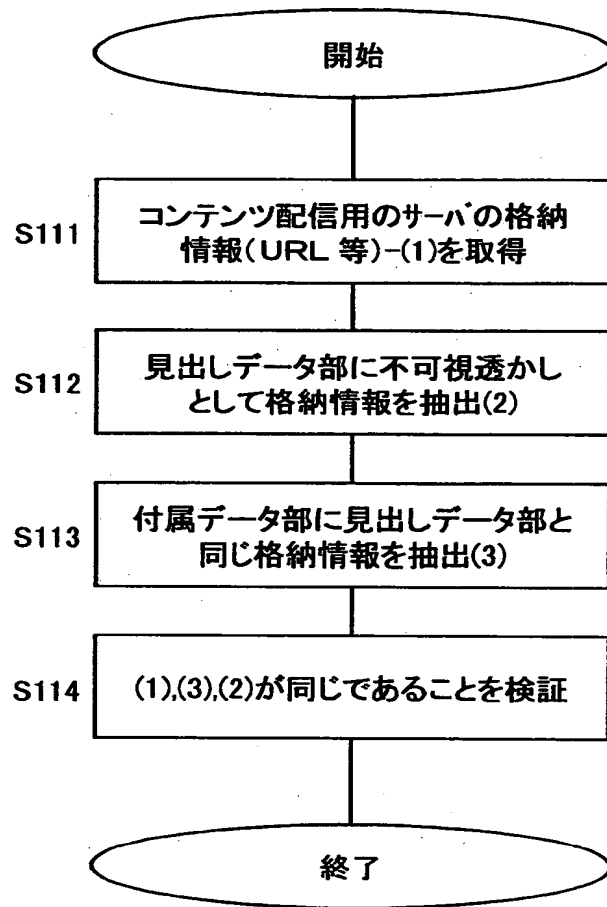
【図 1 6】



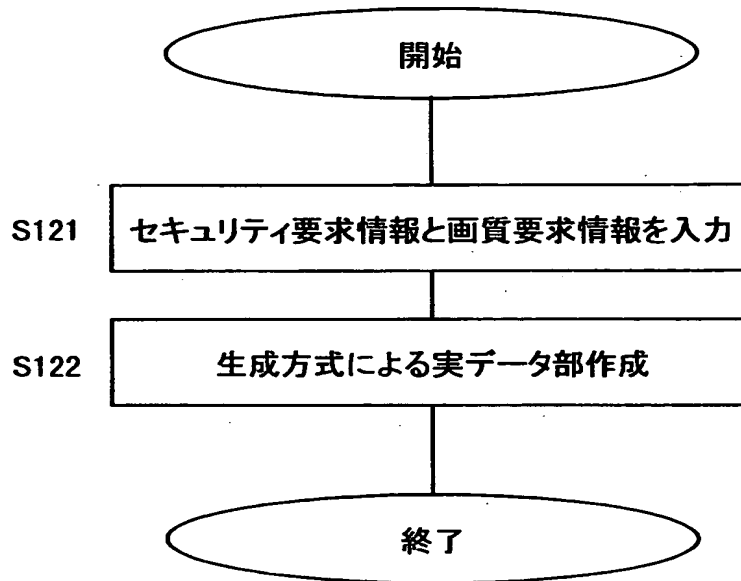
【図 1 7】



【図 1 8】



【図 1 9】



【図 2 0】

画質要求	セキュリティ要求	実データ部の生成例
Low	Low	不可視透かし, 暗号化無
Low	High	不可視透かし, 暗号化有
High	Low	透かし不要, 暗号化無
High	High	可視透かし, 暗号化有

【書類名】 要約書

【要約】

【課題】 デジタルコンテンツを暗号化して配布することで著作権の侵害を防止するとともに、データ中に含まれているデジタルコンテンツがどのような内容であるかを把握することが容易であるようなデータ運用方法を提供する。

【解決手段】 配布を行うデジタルコンテンツの内容を視覚的または聴覚的に認識できるようにシンボル化したシンボル情報を生成し（ステップ S 1 2）、シンボル情報を見出しデータ部に埋め込み（ステップ S 1 3）、デジタルコンテンツを暗号化し（ステップ S 1 5）、コンテンツ鍵の情報を含む許諾情報を電子透かしとして見出しデータ部に埋め込み（ステップ S 1 6）、実データ部と許諾情報付見出しデータ部とを合成して配布する（ステップ S 1 7）。

【選択図】 図 6

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日
[変更理由] 住所変更
住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社